

1 John J. Nelson (SBN 317598)  
2 **MILBERG COLEMAN BRYSON**  
3 **PHILLIPS GROSSMAN, LLC**  
4 280 S. Beverly Drive  
Beverly Hills, CA 90212  
Tel: (858) 209-6941  
Email: [jnelson@milberg.com](mailto:jnelson@milberg.com)

6 William B. Federman\*  
7 **FEDERMAN & SHERWOOD**  
8 10205 N. Pennsylvania Ave.  
Oklahoma City, OK 73120  
9 Telephone: (405) 235-1560  
Fax: (405) 239-2112  
Email: [wbf@federmanlaw.com](mailto:wbf@federmanlaw.com)

11 \**Pro Hac Vice* application to be submitted

13 ***Counsel for Plaintiff and the Proposed Class***

14  
15                   **UNITED STATES DISTRICT COURT**  
                 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**

16                   **VICTORIA MINNICH**, individually  
17 and on behalf of all other similarly  
18 situated individuals,

19                   Plaintiff,

20                   v.  
21                   **EP GLOBAL PRODUCTION**  
                 **SOLUTIONS, LLC D/B/A**  
                 **ENTERTAINMENT PARTNERS**,

23                   Defendant.

Case No. \_\_\_\_\_  
**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

1 Plaintiff Victoria Minnich (“Plaintiff”), individually and on behalf of all  
2 others similarly situated, brings this Class Action lawsuit, against EP Global  
3 Production Solutions, LLC d/b/a Entertainment Partners (“EP” or “Defendant”)  
4 based on personal knowledge and the investigation of her counsel, and alleges as  
5 follows:

6 **I. INTRODUCTION**

7 1. With this action, Plaintiff seeks to hold Defendant responsible for the  
8 harms it caused Plaintiff and approximately **471,362** similarly situated persons in  
9 the massive and preventable data breach of Defendant’s inadequately protected  
10 computer network.

11 2. On June 30, 2023, EP detected suspicious activity on certain systems  
12 within its computer network that supported a subset of accounting applications.<sup>1</sup>  
13 Following an investigation, EP Software determined that a threat actor acquired EP  
14 files containing the personal information of Plaintiff and the Class (the “Data  
15 Breach” or “Breach”).<sup>2</sup>

16 3. According to EP, the personal information exposed, copied, and  
17 acquired by cybercriminals includes names, mailing addresses, Social Security  
18 numbers and/or tax identification numbers (collectively, “PII,” “Personally  
19 Identifiable Information,” “Private Information,” or “Personal Information”).<sup>3</sup>

20 4. EP is a business services company based in Burbank California that  
21 serves clients in the production management space, providing payroll, workforce  
22 management, residuals, tax incentives, finance, and other services.<sup>4</sup> Entertainment

23  
24  
25 <sup>1</sup> See Exhibit 1.

26 <sup>2</sup> *Id.*

27 <sup>3</sup> *Id.*

28 <sup>4</sup> See <https://www.jdsupra.com/legalnews/entertainment-partners-notifies-471k-of-3579067/>.

1 Partners also developed SmartAccounting, a production accounting software, and  
2 operates Central Casting, a leading background actor database.<sup>5</sup>

3 5. As part of its business, and in order to gain profits, EP collected,  
4 obtained, and stored the PII of Plaintiff and the Class.

5 6. By taking possession and control of Plaintiff's and Class Members'  
6 Personal Information, Defendant assumed a duty to securely store and protect the  
7 Personal Information of Plaintiff and the Class.

8 7. Defendant breached this duty and betrayed the trust of Plaintiff and  
9 Class Members by failing to properly safeguard and protect their Personal  
10 Information, thus enabling cyber criminals to access, acquire, copy, appropriate,  
11 compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

12 8. Defendant's misconduct – failing to implement adequate and  
13 reasonable measures to protect Plaintiff's and Class Members' Personal  
14 Information, failing to timely detect the Data Breach, failing to take adequate steps  
15 to prevent and stop the Data Breach, failing to disclose the material facts that it did  
16 not have adequate security practices in place to safeguard the Personal Information,  
17 and failing to provide timely and adequate notice of the Data Breach – caused  
18 substantial harm and injuries to Plaintiff and Class Members across the United  
19 States.

20 9. Due to Defendant's negligence and failures, cyber criminals obtained  
21 and now possess everything they need to commit personal and medical identity theft  
22 and wreak havoc on the financial and personal lives of **more than 470,000**  
23 **individuals**, for decades to come.<sup>6</sup>

24 10. Plaintiff brings this class action lawsuit to hold Defendant responsible  
25 for its grossly negligent—indeed, reckless—failure to use statutorily required or  
26

---

27 <sup>5</sup> *Id.*

28 <sup>6</sup> See <https://apps.web.main.gov/online/aevIEWER/ME/40/6dd29d7e-9e44-4ad0-9d48-1e0bd6122ab6.shtml>.

reasonable industry cybersecurity measures to protect Class Members' Personal Information.

11. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiff and Class Members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class Members are now forced to deal with the danger of identity thieves possessing and using their Personal Information.

12. Additionally, Plaintiff and Class Members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

13. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages and restitution. Plaintiff also seeks declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper.

## II. THE PARTIES

14. Plaintiff is domiciled in the State of California.

15. Defendant is a Delaware limited liability company with its principal place of business located at 2950 North Hollywood Way, Burbank, California 91505.

### **III. JURISDICTION AND VENUE**

16. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

17. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 Class Members, the amount in controversy exceeds

1 \$5,000,000, exclusive of interest and costs, and Plaintiff and members of the Class  
2 are citizens of states that differ from Defendant.<sup>7</sup>

3       18. This Court has personal jurisdiction over Defendant because  
4 Defendant conducts business in and has sufficient minimum contacts with this  
5 District.

6       19. Venue is likewise proper as to Defendant in this District under 28  
7 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this  
8 District and many of Defendant's acts complained of herein occurred within this  
9 District.

10                          **IV. FACTUAL ALLEGATIONS**

11                          **A. THE DATA BREACH AND DEFENDANT'S BELATED  
12 NOTICE.**

13       20. On June 30, 2023, EP discovered third-party cyber criminals  
14 conducted a successful cybersecurity attack whereby they infiltrated Defendant's  
15 inadequately protected systems and gained unauthorized access to the confidential  
16 Personal Information of hundreds of thousands of individuals whose data was stored  
17 within Defendant's system.<sup>8</sup>

18       21. Defendant does not disclose when the Data Breach began nor when it  
19 ended. The only information provided is that the Breach was discovered June 30,  
20 2023.<sup>9</sup> Based on the sparse information provided, it is apparent that cybercriminals  
21 were able to roam Defendant's systems without detection or interference for quite  
22 some time.

23       22. Following an investigation, it was determined that the cybercriminals  
24 acquired files containing the Personal Information of Plaintiff and the Class,

---

25  
26       <sup>7</sup> See *id.*

27       <sup>8</sup> *Id.*

28       <sup>9</sup> See Exhibit 1.

1 approximately **471,362** individuals.<sup>10</sup> While EP discovered the Data Breach on June  
2 30, 2023, it did not begin notifying Plaintiff and the Class until on or around August  
3 1, 2023.<sup>11</sup>

4 23. The types of Personal Information accessed by the unauthorized actor  
5 include names, mailing addresses, Social Security numbers and/or tax identification  
6 numbers.<sup>12</sup>

7 24. Based on the Notice of Security Breach letter (“Notice Letter”)  
8 received by Plaintiff, which specifically states the threat actor **acquired** data base  
9 files containing Plaintiff and the Class’s PII, it is evident Plaintiff and the Class’s  
10 PII was stolen and is in the hands of cybercriminals.<sup>13</sup>

11 25. Defendant had obligations created by industry standards, common law,  
12 statutory law, and its own assurances and representations to keep Plaintiff’s and  
13 Class Members’ Personal Information confidential and to protect such Personal  
14 Information from unauthorized access.

15 26. Nevertheless, Defendant failed to spend sufficient resources on  
16 preventing external access, detecting outside infiltration, and training its employees  
17 to identify threats and defend against them.

18 27. The stolen Personal Information at issue has great value to the hackers,  
19 due to the large number of individuals affected and the fact that Social Security  
20 numbers were part of the data that was compromised.

21  
22  
23  
24

---

<sup>10</sup> See <https://apps.web.main.gov/online/aeviwer/ME/40/6dd29d7e-9e44-4ad0-9d48-1e0bd6122ab6.shtml>.

25  
26<sup>11</sup> *Id.*

27<sup>12</sup> See Exhibit 1.

28<sup>13</sup> *Id.*

1           **B. PLAINTIFF'S EXPERIENCE.**

2       28. Plaintiff entrusted her Private Information to one of the entities that  
 3 contracts services from EP. Upon information and belief, EP's agreements with  
 4 those entities required it to protect and maintain the confidentiality of the Private  
 5 Information entrusted to it. EP expressly encouraged Plaintiff and the Class to  
 6 provide their PII to EP for direct deposit purposes.

7       29. Plaintiff received a Notice Letter from Defendant dated August 1,  
 8 2023, informing her that her Personal Information, including her name, mailing  
 9 address, Social Security number and/or tax identification number was specifically  
 10 identified as having been compromised and acquired in the Data Breach.<sup>14</sup> Plaintiff  
 11 reasonably fears additional PII may have been exposed beyond what Defendant  
 12 states in the Notice Letter.

13      30. Plaintiff and Class members' PII was entrusted to Defendant with the  
 14 reasonable expectation and mutual understanding that Defendant would comply  
 15 with its obligations to keep such information confidential and secure from  
 16 unauthorized access. Plaintiff would not have provided her PII to EP had she known  
 17 that would not undertake reasonable data security measures.

18      31. Because of the Data Breach, Plaintiff's Personal Information is now in  
 19 the hands of cybercriminals. Plaintiff and all Class Members are now imminently  
 20 at risk of crippling future identity theft and fraud.

21      32. As a result of the Data Breach, Plaintiff has already expended time and  
 22 suffered loss of productivity from taking time to address and attempt to ameliorate,  
 23 mitigate, and address the future consequences of the Data Breach, including  
 24 investigating the Data Breach, investigating how best to ensure that she is protected  
 25 from identity theft, and reviewing account statements and other information.

---

26  
 27  
 28      <sup>14</sup> *Id.*

1       33. Plaintiff has also suffered injury directly and proximately caused by  
2 the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information;  
3 (b) the imminent and certain impending injury flowing from fraud and identity theft  
4 posed by Plaintiff's Personal Information being placed in the hands of cyber  
5 criminals; (c) damages to and diminution in value of Plaintiff's Personal  
6 Information that was entrusted to Defendant for with the understanding that  
7 Defendant would safeguard this information against disclosure; (d) loss of the  
8 benefit of the bargain with Defendant to provide adequate and reasonable data  
9 security—*i.e.*, the difference in value between what Plaintiff should have received  
10 from Defendant and Defendant's defective and deficient performance of that  
11 obligation by failing to provide reasonable and adequate data security and failing to  
12 protect Plaintiff's Personal Information; and (e) continued risk to Plaintiff's  
13 Personal Information, which remains in the possession of Defendant and which is  
14 subject to further breaches so long as Defendant fails to undertake appropriate and  
15 adequate measures to protect the Personal Information that was entrusted to  
16 Defendant.

17       **C. DEFENDANT HAD AN OBLIGATION TO PROTECT  
18 PERSONAL INFORMATION UNDER THE LAW AND THE  
APPLICABLE STANDARD OF CARE.**

19       34. Defendant was prohibited by the Federal Trade Commission Act (the  
20 “FTC Act”) (15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices  
21 in or affecting commerce.” The Federal Trade Commission (the “FTC”) has  
22 concluded that a company’s failure to maintain reasonable and appropriate data  
23 security for consumers’ sensitive personal information is an “unfair practice” in  
24 violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d  
25 236 (3d Cir. 2015).

26       35. Defendant is further required by various states’ laws and regulations to  
27 protect Plaintiff’s and Class Members’ Personal Information.

1       36. Defendant owed a duty to Plaintiff and the Class to design, maintain,  
2 and test its computer systems and applications to ensure that the Personal  
3 Information in its possession was adequately secured and protected.

4       37. Defendant owed a duty to Plaintiff and the Class to create and  
5 implement reasonable data security practices and procedures to protect the Personal  
6 Information in its possession, including adequately training its employees (and  
7 others who accessed Personal Information within its computer systems) on how to  
8 adequately protect Personal Information.

9       38. Defendant owed a duty to Plaintiff and the Class to implement  
10 processes that would detect a breach of its systems in a timely manner.

11       39. Defendant owed a duty to Plaintiff and the Class to act upon data  
12 security warnings and alerts in a timely fashion.

13       40. Defendant owed a duty to Plaintiff and the Class to disclose if its  
14 computer systems and data security practices were inadequate to safeguard  
15 individuals' Personal Information from theft because such an inadequacy would be  
16 a material fact in the decision to entrust Personal Information with Defendant.

17       41. Defendant owed a duty to Plaintiff and the Class to disclose in a timely  
18 and accurate manner when data breaches occurred.

19       42. Defendant owed a duty of care to Plaintiff and the Class because they  
20 were foreseeable and probable victims of any inadequate data security practices.

21       **D. DEFENDANT WAS ON NOTICE OF CYBER ATTACK  
22           THREATS AND OF THE INADEQUACY OF THEIR DATA  
23           SECURITY**

24       43. Data security breaches have dominated the headlines for the last two  
25 decades and it does not take an IT industry expert to recognize this. The general  
26 public is well-aware of the names of some of the biggest cybersecurity breaches

1 thus far, including – Target,<sup>15</sup> Yahoo!,<sup>16</sup> Marriott International,<sup>17</sup> Chipotle, Chili's,  
 2 Arby's,<sup>18</sup> and many others.<sup>19</sup>

3       44. Defendant should certainly have been aware, and indeed was aware,  
 4 that it was at risk for a data breach that could expose the PII it collected and  
 5 maintained.

6       45. Defendant was also on notice of the importance of data encryption of  
 7 Personal Information. Defendant knew it kept Personal Information in its systems  
 8 and yet it appears Defendant did not encrypt these systems or the information  
 9 contained within them.

10      46. Defendant should have known about its data security weaknesses and  
 11 sought better protection for the Personal Information maintained on its systems.

16      15 Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and*  
 17 *Lessons Learned*, ZDNET (Feb. 2, 2015), <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/>.

19      16 Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*,  
 CSOONLINE.COM (Oct. 4, 2017), <https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html>.

21      17 Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE:  
 22 HASHEDOUT (Mar. 22, 2019), <https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/>.

24      18 Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), <https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b>.

26      19 See, e.g., Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO  
 27 ONLINE (Dec. 20, 2018), <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

1           **E. CYBER CRIMINALS WILL USE PLAINTIFF'S AND CLASS  
2           MEMBERS' PERSONAL INFORMATION TO DEFRAUD  
3           THEM.**

4       47. Plaintiff and Class Members' Personal Information is of great value to  
5       hackers and cyber criminals, and the data stolen in the Data Breach has been used  
6       and will continue to be used in a variety of sordid ways for criminals to exploit  
7       Plaintiff and the Class Members and to profit off their misfortune.

8       48. Each year, identity theft causes tens of billions of dollars of losses to  
9       victims in the United States.<sup>20</sup> For example, with the Personal Information stolen in  
10      the Data Breach identity thieves can open financial accounts, apply for credit, file  
11      fraudulent tax returns, commit crimes, create false driver's licenses and other forms  
12      of identification and sell them to other criminals or undocumented immigrants, steal  
13      government benefits, give breach victims' names to police during arrests, and many  
14      other harmful forms of identity theft.<sup>21</sup> These criminal activities have and will result  
15      in devastating financial and personal losses to Plaintiff and Class Members.

16       49. Personal Information is such a valuable commodity to identity thieves  
17      that once it has been compromised, criminals will use it and trade the information  
18      on the cyber black-market for years.<sup>22</sup> For example, it is believed that certain  
19      Personal Information compromised in the 2017 Experian data breach was being

---

20       <sup>20</sup> "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst.,  
21       <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing  
22       Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of  
Complexity").

23  
24       <sup>21</sup>See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security*  
Number, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

25  
26       <sup>22</sup> *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;*  
However, the Full Extent Is Unknown, GAO, July 5, 2007,  
<https://www.gao.gov/assets/270/262904.html>.

1 used, three years later, by identity thieves to apply for COVID-19-related benefits  
 2 in the state of Oklahoma.<sup>23</sup>

3       50. Based on the foregoing, the information compromised in the Data  
 4 Breach is significantly more valuable than the loss of, for example, credit card  
 5 information in a retailer data breach because there, victims can cancel or close credit  
 6 and debit card accounts. The information compromised in this Data Breach is  
 7 impossible to “close” and difficult, if not impossible, to change—Social Security  
 8 number and name.

9       51. This data demands a much higher price on the black market. Martin  
 10 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to  
 11 credit card information, personally identifiable information and Social Security  
 12 numbers are worth more than 10x on the black market.<sup>24</sup>

13       52. This was a financially motivated Data Breach, as apparent from the  
 14 discovery of the cybercriminals seeking to profit off the sale of Plaintiff’s and the  
 15 Class Members’ Personal Information on the dark web. The Personal Information  
 16 exposed in this Data Breach is valuable to identity thieves for use in the kinds of  
 17 criminal activity described herein.

---

18  
 19  
 20  
 21  
 22

23 <sup>23</sup>See <https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html>; see also <https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/>.

24 <sup>24</sup> Tim Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolensells-for-10x-price-of-stolen-credit-card-numbers.html>.

1       53. These risks are both certainly impending and substantial. As the FTC  
 2 has reported, if hackers get access to personally identifiable information, they will  
 3 use it.<sup>25</sup>

4       54. Hackers may not use the accessed information right away. According  
 5 to the U.S. Government Accountability Office, which conducted a study regarding  
 6 data breaches:

7           [In some cases, stolen data may be held for up to a year or more  
 8 before being used to commit identity theft. Further, once stolen  
 9 data have been sold or posted on the Web, fraudulent use of that  
 10 information may continue for years. As a result, studies that  
 11 attempt to measure the harm resulting from data breaches cannot  
 necessarily rule out all future harm.]<sup>26</sup>

12       55. As described above, identity theft victims must spend countless hours  
 13 and large amounts of money repairing the impact to their credit.<sup>27</sup>

14       56. With this Data Breach, identity thieves have already started to prey on  
 15 the victims, and one can reasonably anticipate this will continue.

16       57. Victims of the Data Breach, like Plaintiff and other Class Members,  
 17 must spend many hours and large amounts of money protecting themselves from  
 18 the current and future negative impacts to their credit because of the Data Breach.<sup>28</sup>

19       58. In fact, as a direct and proximate result of the Data Breach, Plaintiff  
 20 and the Class have suffered, and have been placed at an imminent, immediate, and

---

22       <sup>25</sup>Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM’N (May  
 23 24, 2017), <https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

24       <sup>26</sup>*Data Breaches Are Frequent*, *supra* note 22.

25       <sup>27</sup> “Guide for Assisting Identity Theft Victims,” Federal Trade Commission, 4 (Sept.  
 26 2013), <http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf>.

28       <sup>28</sup>*Id.*

1 continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff  
2 and the Class must now take the time and effort and spend the money to mitigate  
3 the actual and potential impact of the Data Breach on their everyday lives, including  
4 purchasing identity theft and credit monitoring services, placing “freezes” and  
5 “alerts” with credit reporting agencies, contacting their financial institutions,  
6 healthcare providers, closing or modifying financial accounts, and closely  
7 reviewing and monitoring bank accounts, credit reports, and health insurance  
8 account information for unauthorized activity for years to come.

9 59. Plaintiff and the Class have suffered, and continue to suffer, actual  
10 harms for which they are entitled to compensation, including:

- 11 a. Trespass, damage to, and theft of their personal property  
12 including Personal Information;
- 13 b. Improper disclosure of their Personal Information;
- 14 c. The imminent and certainly impending injury flowing from  
15 potential fraud and identity theft posed by their Personal  
16 Information being placed in the hands of criminals and having  
17 been already misused;
- 18 d. The imminent and certainly impending risk of having their  
19 Personal Information used against them by spam callers to  
20 defraud them;
- 21 e. Damages flowing from Defendant’s untimely and inadequate  
22 notification of the data breach;
- 23 f. Loss of privacy suffered as a result of the Data Breach;
- 24 g. Ascertainable losses in the form of out-of-pocket expenses and  
25 the value of their time reasonably expended to remedy or  
26 mitigate the effects of the data breach;
- 27 h. Ascertainable losses in the form of deprivation of the value of  
28 Plaintiff’s and the Class’s personal information for which there

1                   is a well-established and quantifiable national and international  
2                   market;

3                   i.       The loss of use of and access to their credit, accounts, and/or  
4                   funds;  
5                   j.       Damage to their credit due to fraudulent use of their Personal  
6                   Information; and  
7                   k.       Increased cost of borrowing, insurance, deposits and other items  
8                   which are adversely affected by a reduced credit score.

9         60.   Moreover, Plaintiff and Class Members have an interest in ensuring  
10      that their information, which remains in the possession of Defendant, is protected  
11      from further breaches by the implementation of industry standard and statutorily  
12      compliant security measures and safeguards. Defendant has shown itself to be  
13      incapable of protecting Plaintiff's and Class Members' Personal Information.

14         61.   Plaintiff and Class Members are desperately trying to mitigate the  
15      damage that Defendant has caused them but, given the Personal Information  
16      Defendant made accessible to hackers, they are certain to incur additional damages.  
17      Because identity thieves have their Personal Information, Plaintiff and all Class  
18      Members will need to have identity theft monitoring protection for the rest of their  
19      lives. Some may even need to go through the long and arduous process of getting a  
20      new Social Security number, with all the loss of credit and employment difficulties  
21      that come with this change.<sup>29</sup>

22  
23  
24  
25  
26         

---

<sup>29</sup>*Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16,  
27         2015), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html>.

1       62. None of this should have happened. The Data Breach was preventable.

2       **F. DEFENDANT COULD HAVE PREVENTED THE DATA  
3           BREACH BUT FAILED TO ADEQUATELY PROTECT  
4           PLAINTIFF'S AND CLASS MEMBERS' PERSONAL  
5           INFORMATION.**

6       63. Data breaches are preventable.<sup>30</sup> As Lucy Thompson wrote in the  
7     DATA BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data  
8     breaches that occurred could have been prevented by proper planning and the  
9     correct design and implementation of appropriate security solutions.”<sup>31</sup> She added  
10    that “[o]rganizations that collect, use, store, and share sensitive personal data must  
11    accept responsibility for protecting the information and ensuring that it is not  
12    compromised . . .”<sup>32</sup>

13      64. “Most of the reported data breaches are a result of lax security and the  
14    failure to create or enforce appropriate security policies, rules, and procedures ...  
15    Appropriate information security controls, including encryption, must be  
16    implemented and enforced in a rigorous and disciplined manner so that a *data  
17    breach never occurs.*”<sup>33</sup>

18      65. The FTC has promulgated numerous guides for businesses which  
19    highlight the importance of implementing reasonable data security practices.  
20    According to the FTC, the need for data security should be factored into all business  
21    decision-making.

22      66. In 2016, the FTC updated its publication, *Protecting Personal  
23    Information: A Guide for Business*, which established cyber-security guidelines for

---

24      <sup>30</sup>Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” in  
25    DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

26      <sup>31</sup>*Id.* at 17.

27      <sup>32</sup>*Id.* at 28.

28      <sup>33</sup>*Id.*

1 businesses. The guidelines note that businesses should protect the personal  
 2 customer information that they keep; properly dispose of personal information that  
 3 is no longer needed; encrypt information stored on computer networks; understand  
 4 their network's vulnerabilities; and implement policies to correct any security  
 5 problems.<sup>34</sup> The guidelines also recommend that businesses use an intrusion  
 6 detection system to expose a breach as soon as it occurs; monitor all incoming traffic  
 7 for activity indicating someone is attempting to hack the system; watch for large  
 8 amounts of data being transmitted from the system; and have a response plan ready  
 9 in the event of a breach.<sup>35</sup>

10       67. The FTC further recommends that companies not maintain PII longer  
 11 than is needed for authorization of a transaction; limit access to sensitive data;  
 12 require complex passwords to be used on networks; use industry-tested methods for  
 13 security; monitor for suspicious activity on the network; and verify that third-party  
 14 service providers have implemented reasonable security measures.

15       68. The FTC has brought enforcement actions against businesses for  
 16 failing to adequately and reasonably protect customer data, treating the failure to  
 17 employ reasonable and appropriate measures to protect against unauthorized access  
 18 to confidential consumer data as an unfair act or practice prohibited by Section 5 of  
 19 the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting  
 20 from these actions further clarify the measures businesses must take to meet their  
 21 data security obligations.

22       69. These FTC enforcement actions include actions against healthcare  
 23 providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A*  
 24

---

25  
 26<sup>34</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission  
 27 (2016), available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_protecting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf).

28<sup>35</sup> *Id.*

1 *Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at \*32 (MSNET July  
 2 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices  
 3 were unreasonable and constitute an unfair act or practice in violation of Section 5  
 4 of the FTC Act.”).

5       70. Defendant failed to properly implement basic data security practices,  
 6 including those set forth by the FTC.

7       71. Defendant’s failure to employ reasonable and appropriate measures to  
 8 protect against unauthorized access to customers’ Personal Information constitutes  
 9 an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

10     72. Defendant also failed to meet the minimum standards of any of the  
 11 following frameworks: the NIST Cybersecurity Framework Version 1.1 (including  
 12 without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7,  
 13 PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7,  
 14 DE.CM-8, and RS.CO-2), and the Center for Internet Security’s Critical Security  
 15 Controls (CIS CSC), which are all established standards in reasonable cybersecurity  
 16 readiness.

17     73. Defendant was entrusted with properly holding, safeguarding, and  
 18 protecting against unlawful disclosure of Plaintiff’s and the Class’s Personal  
 19 Information.

20     74. Many failures laid the groundwork for the success (“success” from a  
 21 cybercriminal’s viewpoint) of the Data Breach, starting with Defendant’s failure to  
 22 incur the costs necessary to implement adequate and reasonable cyber security  
 23 procedures and protocols necessary to protect Plaintiff’s and Class Members’  
 24 Personal Information.

25     75. Defendant was at all times fully aware of its obligation to protect the  
 26 Personal Information of Plaintiff and Class Members. Defendant was also aware of  
 27 the significant repercussions that would result from its failure to do so.

76. Defendant maintained the Personal Information in a reckless manner. In particular, the Personal Information was maintained and/or exchanged, unencrypted, in Defendant's business email accounts that were maintained in a condition vulnerable to cyberattacks.

77. Defendant knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if Plaintiff's and Class Members' Personal Information was stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach.

78. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class Members' Personal Information from those risks left that information in a dangerous condition.

79. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

## **V. CLASS ACTION ALLEGATIONS**

80. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

1       81. Plaintiff brings all claims as class claims under Federal Rule of Civil  
2 Procedure 23. Plaintiff asserts all claims on behalf of the Classes, defined as  
3 follows:

4                   **Nationwide Class**

5       All persons residing in the United States whose personal  
6 information was compromised as a result of the EP Data Breach  
7 and received a Notice Letter.

8                   **California Subclass:**

9       All persons residing in the State of California whose personal  
10 information was compromised as a result of the EP Data Breach  
11 and received a Notice Letter.

12      82. Plaintiff reserves the right to amend the above definitions or to propose  
13 alternative or add subclasses in subsequent pleadings and motions for class  
14 certification.

15      83. The proposed Nationwide Class and Subclass (collectively referred to  
16 herein as the “Class” unless otherwise specified) meet the requirements of Fed. R.  
17 Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

18      84. **Numerosity:** The proposed Class is believed to be so numerous that  
19 joinder of all members is impracticable. The proposed Subclass is also believed to  
20 be so numerous that joinder of all members would be impractical.

21      85. **Typicality:** Plaintiff’s claims are typical of the claims of the Class.  
22 Plaintiff and all members of the Class were injured through Defendant’s uniform  
23 misconduct. The same event and conduct that gave rise to Plaintiff’s claims are  
24 identical to those that give rise to the claims of every other Class Member because  
25 Plaintiff and each member of the Class had their sensitive Personal Information  
26 compromised in the same way by the same conduct of Defendant.

27      86. **Adequacy:** Plaintiff is an adequate representative of the Class because  
28 her interests do not conflict with the interests of the Class and proposed Subclass

1 that she seeks to represent; Plaintiff has retained counsel competent and highly  
 2 experienced in data breach class action litigation; and Plaintiff and Plaintiff's  
 3 counsel intend to prosecute this action vigorously. The interests of the Class will be  
 4 fairly and adequately protected by Plaintiff and her counsel.

5       **87. Superiority:** A class action is superior to other available means of fair  
 6 and efficient adjudication of the claims of Plaintiff and the Class. The injury  
 7 suffered by each individual Class Member is relatively small in comparison to the  
 8 burden and expense of individual prosecution of complex and expensive litigation.  
 9 It would be very difficult, if not impossible, for members of the Class individually  
 10 to effectively redress Defendant's wrongdoing. Even if Class Members could afford  
 11 such individual litigation, the court system could not. Individualized litigation  
 12 presents a potential for inconsistent or contradictory judgments. Individualized  
 13 litigation increases the delay and expense to all parties, and to the court system,  
 14 presented by the complex legal and factual issues of the case. By contrast, the class  
 15 action device presents far fewer management difficulties and provides benefits of  
 16 single adjudication, economy of scale, and comprehensive supervision by a single  
 17 court.

18       **88. Commonality and Predominance:** There are many questions of law  
 19 and fact common to the claims of Plaintiff and the other members of the Class, and  
 20 those questions predominate over any questions that may affect individual members  
 21 of the Class. Common questions for the Class include:

- 22           a. Whether Defendant engaged in the wrongful conduct alleged  
                 herein;
- 23           b. Whether Defendant failed to adequately safeguard Plaintiff's  
                 and the Class's Personal Information;
- 24           c. Whether Defendant's computer systems and data security  
                 practices used to protect Plaintiff's and Class Members'

1 Personal Information violated the FTC Act, and/or state laws,  
2 and/or Defendant's other duties discussed herein;

3 d. Whether Defendant owed a duty to Plaintiff and the Class to  
4 adequately protect their Personal Information, and whether it  
5 breached this duty;

6 e. Whether Defendant knew or should have known that its  
7 computer and network security systems were vulnerable to a  
8 data breach;

9 f. Whether Defendant's conduct, including its failure to act,  
10 resulted in or was the proximate cause of the Data Breach;

11 g. Whether Defendant breached contractual duties owed to  
12 Plaintiff and the Class to use reasonable care in protecting their  
13 Personal Information;

14 h. Whether Defendant failed to adequately respond to the Data  
15 Breach, including failing to investigate it diligently and notify  
16 affected individuals in the most expedient time possible and  
17 without unreasonable delay, and whether this caused damages  
18 to Plaintiff and the Class;

19 i. Whether Defendant continues to breach duties to Plaintiff and  
20 the Class;

21 j. Whether Plaintiff and the Class suffered injury as a proximate  
22 result of Defendant's negligent actions or failures to act;

23 k. Whether Plaintiff and the Class are entitled to recover damages,  
24 equitable relief, and other relief;

25 l. Whether injunctive relief is appropriate and, if so, what  
26 injunctive relief is necessary to redress the imminent and  
27 currently ongoing harm faced by Plaintiff and members of the  
28 Class and the general public;

- 1 m. Whether Defendant's actions alleged herein constitute gross  
2 negligence; and
- 3 n. Whether Plaintiff and Class Members are entitled to punitive  
4 damages.

5 **VI. CAUSES OF ACTION**

6 **COUNT ONE**  
7 **NEGLIGENCE**

8 **(On Behalf of Plaintiff and the Nationwide Class)**

9 89. Plaintiff incorporates by reference all allegations of the preceding  
10 paragraphs as though fully set forth herein.

11 90. Defendant solicited, gathered, and stored the Personal Information of  
12 Plaintiff and the Class as part of the operation of its business.

13 91. Upon accepting and storing the Personal Information of Plaintiff and  
14 Class Members, Defendant undertook and owed a duty to Plaintiff and Class  
15 Members to exercise reasonable care to secure and safeguard that information and  
16 to use secure methods to do so.

17 92. Defendant had full knowledge of the sensitivity of the Personal  
18 Information, the types of harm that Plaintiff and Class Members could and would  
19 suffer if the Personal Information was wrongfully disclosed, and the importance of  
20 adequate security.

21 93. Plaintiff and Class Members were the foreseeable victims of any  
22 inadequate safety and security practices on the part of Defendant. Plaintiff and the  
23 Class Members had no ability to protect their Personal Information that was in  
24 Defendant's possession. As such, a special relationship existed between Defendant  
25 and Plaintiff and the Class.

26 94. Defendant was well aware of the fact that cyber criminals routinely  
27 target large corporations through cyberattacks in an attempt to steal sensitive  
28 personal and medical information.

95. Defendant owed Plaintiff and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

96. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See Restatement (Second) of Torts § 302B.* Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

97. Defendant had duties to protect and safeguard the Personal Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Personal Information. Additional duties that Defendant owed Plaintiff and the Class include:

- a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' Personal Information was adequately secured from impermissible release, disclosure, and publication;
- b. To protect Plaintiff's and Class Members' Personal Information in its possession by using reasonable and adequate security procedures and systems;

- 1       c. To implement processes to quickly detect a data breach, security  
2              incident, or intrusion involving its business email system,  
3              networks, and servers; and  
4       d. To promptly notify Plaintiff and Class Members of any data  
5              breach, security incident, or intrusion that affected or may have  
6              affected their Personal Information.

7       98. Only Defendant was in a position to ensure that its systems and  
8              protocols were sufficient to protect the Personal Information that Plaintiff and the  
9              Class had entrusted to it.

10      99. Defendant breached its duty of care by failing to adequately protect  
11             Plaintiff's and Class Members' Personal Information. Defendant breached its duties  
12             by, among other things:

- 13       a. Failing to exercise reasonable care in obtaining, retaining  
14              securing, safeguarding, deleting, and protecting the Personal  
15              Information in its possession;
- 16       b. Failing to protect the Personal Information in its possession by  
17              using reasonable and adequate security procedures and systems;
- 18       c. Failing to adequately and properly audit, test, and train its  
19              employees to avoid phishing emails;
- 20       d. Failing to use adequate data security systems;
- 21       e. Failing to adequately and properly audit, test, and train its  
22              employees regarding how to properly and securely transmit and  
23              store Personal Information;
- 24       f. Failing to adequately train its employees to not store Personal  
25              Information longer than absolutely necessary;
- 26       g. Failing to consistently enforce security policies aimed at  
27              protecting Plaintiff's and the Class's Personal Information;

- h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;
- i. Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their Personal Information.

100. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

101. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

102. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Personal Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Personal Information of Plaintiff and Class Members while it was within Defendant's possession and control.

103. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps toward securing their Personal Information and mitigating damages.

104. As a result of the Data Breach, Plaintiff and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and financial account statements.

105. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

1       106. The damages Plaintiff and the Class have suffered (as alleged above)  
 2 and will suffer were and are the direct and proximate result of Defendant's grossly  
 3 negligent conduct.

4       107. In addition to its duties under common law, Defendant had additional  
 5 duties imposed by statute and regulations, including the duties under the FTC Act.  
 6 The harms which occurred as a result of Defendant's failure to observe these duties,  
 7 including the loss of privacy, lost time and expense, and significant risk of identity  
 8 theft are the types of harm that these statutes and regulations intended to prevent.

9       108. Defendant violated these statutes when it engaged in the actions and  
 10 omissions alleged herein, and Plaintiff's and Class Members' injuries were a direct  
 11 and proximate result of Defendant's violations of these statutes. Plaintiff therefore  
 12 is entitled to the evidentiary presumptions for negligence *per se*.

13       109. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to  
 14 Plaintiff and the Class to provide fair and adequate computer systems and data  
 15 security to safeguard the Personal Information of Plaintiff and the Class.

16       110. The FTC Act prohibits "unfair practices in or affecting commerce,"  
 17 including, as interpreted and enforced by the FTC, the unfair act or practice by  
 18 businesses, such as Defendant, of failing to use reasonable measures to protect  
 19 Personal Information. The FTC publications and orders described above also  
 20 formed part of the basis of Defendant's duty in this regard.

21       111. Defendant gathered and stored the Personal Information of Plaintiff  
 22 and the Class as part of its business of soliciting and facilitating its services to its  
 23 clients, which affect commerce.

24       112. Defendant violated the FTC Act by failing to use reasonable measures  
 25 to protect the Personal Information of Plaintiff and the Class and by not complying  
 26 with applicable industry standards, as described herein.

27       113. Defendant breached its duties to Plaintiff and the Class under the FTC  
 28 Act by failing to provide fair, reasonable, or adequate computer systems and/or data

1 security practices to safeguard Plaintiff's and Class Members' Personal  
2 Information, and by failing to provide prompt and specific notice without  
3 reasonable delay.

4 114. Plaintiff and the Class are within the class of persons that the FTC Act  
5 were intended to protect.

6 115. The harm that occurred as a result of the Data Breach is the type of  
7 harm the FTC Act was intended to guard against.

8 116. Defendant breached its duties to Plaintiff and the Class under these  
9 laws by failing to provide fair, reasonable, or adequate computer systems and data  
10 security practices to safeguard Plaintiff's and the Class's Personal Information.

11 117. Defendant breached its duties to Plaintiff and the Class by  
12 unreasonably delaying and failing to provide notice of the Data Breach  
13 expeditiously and/or as soon as practicable to Plaintiff and the Class.

14 118. As a direct and proximate result of Defendant's negligence, Plaintiff  
15 and the Class have suffered, and continue to suffer, damages arising from the Data  
16 Breach, as alleged above.

17 119. The injury and harm that Plaintiff and Class Members suffered (as  
18 alleged above) was the direct and proximate result of Defendant's negligence.

19 120. Plaintiff and the Class have suffered injury and are entitled to actual  
20 and punitive damages in amounts to be proven at trial.

21 **COUNT TWO**  
22 **UNJUST ENRICHMENT**  
23 **(On Behalf of Plaintiff and the Nationwide Class)**

24 121. Plaintiff incorporates by reference all allegations of the preceding  
25 paragraphs as though fully set forth herein.

26 122. Plaintiff and the Class bring this claim in the alternative to all other  
27 claims and remedies at law.

1       123. Through and as a result of Plaintiff and Class members' use of  
2 Defendant's services - directly or indirectly through the entities to whom Plaintiff  
3 and Class Members entrusted their Personal Information with and who subsequently  
4 transmitted that Personal Information to Defendant - Defendant received monetary  
5 benefits and the use of the valuable Personal Information for business purposes and  
6 financial gain.

7       124. Defendant collected, maintained, and stored the Personal Information  
8 of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the  
9 monetary benefits conferred upon it (including the use of valuable Personal  
10 Information for business purposes and financial gain) by the entities that collected  
11 Plaintiff's and Class members' Personal Information and that used Defendant's  
12 services.

13       125. Defendant, by way of its affirmative actions and omissions, including  
14 its knowing violations of its express or implied contracts with the entities that  
15 collected Plaintiff's and Class Members' Personal Information, knowingly and  
16 deliberately enriched itself by saving the costs it reasonably and contractually  
17 should have expended on reasonable data privacy and security measures to secure  
18 Plaintiff's and Class Members' Personal Information.

19       126. Instead of providing a reasonable level of security, training, and  
20 protocols that would have prevented the Data Breach, as described above and as is  
21 common industry practice among companies entrusted with similar Personal  
22 Information, Defendant, upon information and belief, instead consciously, and  
23 opportunistically calculated to increase its own profits at the expense of Plaintiff  
24 and Class Members.

25       127. As a direct and proximate result of Defendant's decision to profit rather  
26 than provide adequate data security, Plaintiff and Class Members suffered and  
27 continue to suffer actual damages, including (i) the amount of the savings and costs  
28 Defendant reasonably and contractually should have expended on data security

measures to secure Plaintiff's Personal Information, (ii) time and expenses mitigating harms, (iii) diminished value of Personal Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

128. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

129. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

**COUNT THREE**  
**BREACH OF THIRD-PARTY BENEFICIARY CONTRACT**  
**On Behalf of Plaintiff and the Nationwide Class**

130. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

131. Defendant entered into contracts, written or implied, with its clients to perform services that include, but are not limited to, providing staffing software and other services. Upon information and belief, these contracts are virtually identical between and among Defendant and its customers around the country whose employees were affected by the Data Breach.

132. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiff and the Class.

133. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class members were the intended third-party beneficiaries

1 of the contracts entered into between Defendant and its clients. Defendant knew that  
2 if it were to breach these contracts with its clients, the clients' employees—Plaintiff  
3 and Class members—would be harmed.

4 134. Defendant breached the contracts it entered into with its clients by,  
5 among other things, failing to (i) use reasonable data security measures, (ii)  
6 implement adequate protocols and employee training sufficient to protect Plaintiff's  
7 PII from unauthorized disclosure to third parties, and (iii) promptly and adequately  
8 notify Plaintiff and Class Members of the Data Breach.

9 135. Plaintiff and the Class were harmed by Defendant's breach of its  
10 contracts with its clients, as such breach is alleged herein, and are entitled to the  
11 losses and damages they have sustained as a direct and proximate result thereof.

12 136. Plaintiff and Class Members are also entitled to their costs and  
13 attorney's fees incurred in this action.

14 **COUNT FOUR**  
15 **VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT**  
16           **Cal. Civ. Code §§ 1798.80, *et seq.***  
17           **(on behalf of Plaintiff and the California Subclass)**

18 137. Plaintiff, individually and on behalf of the California Subclass, repeats  
19 and alleges the foregoing allegations as if fully alleged herein.

20       138. “[T]o ensure that Personal Information about California residents is  
21 protected,” the California legislature enacted Cal. Civ. Code § 1798.81.5, which  
22 requires that any business that “owns, licenses, or maintains Personal Information  
23 about a California resident shall implement and maintain reasonable security  
24 procedures and practices appropriate to the nature of the information, to protect the  
25

1 Personal Information from unauthorized access, destruction, use, modification, or  
2 disclosure.”  
3

4       139. Defendant is a business that owns, maintains, and licenses Personal  
5 Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and  
6 California Subclass Members.  
7

8       140. Businesses that own or license computerized data that includes  
9 Personal Information are required to notify California residents when their Personal  
10 Information has been acquired (or is reasonably believed to have been acquired) by  
11 unauthorized persons in a data security breach “in the most expedient time possible  
12 and without unreasonable delay.” Cal. Civ. Code § 1798.82. Among other  
13 requirements, the security breach notification must include “the types of Personal  
14 Information that were or are reasonably believed to have been the subject of the  
15 Information that were or are reasonably believed to have been the subject of the  
16 breach.” Cal. Civ. Code § 1798.82.  
17

18       141. Defendant is a business that owns or licenses computerized data that  
19 includes Personal Information as defined by Cal. Civ. Code § 1798.82.  
20

21       142. Plaintiff and California Subclass Members’ Personal Information  
22 includes Personal Information as covered by Cal. Civ. Code § 1798.82.  
23

24       143. Because Defendant reasonably believed that Plaintiff’s and California  
25 Subclass Members’ Personal Information was acquired by unauthorized persons  
26 during the Data Breach, Defendant had an obligation to disclose the Data Breach in  
27 a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.  
28

1           144. By failing to disclose the Data Breach in a timely and accurate manner,  
2 Defendant violated Cal. Civ. Code § 1798.82.  
3

4           145. As a direct and proximate result of Defendant's violations of the Cal.  
5 Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass Members  
6 suffered damages, as described above.  
7

8           146. Plaintiff and California Subclass Members seek relief under Cal. Civ.  
9 Code § 1798.84, including actual damages and injunctive relief.  
10

## **VII. PRAYER FOR RELIEF**

11           WHEREFORE, Plaintiff and the Class pray for judgment against Defendant  
12 as follows:  
13

- 14           a. An order certifying this action as a class action under Fed. R.  
15           Civ. P. 23, defining the Class as requested herein, appointing the  
16           undersigned as Class counsel, and finding that Plaintiff is a  
17           proper representative of the Class requested herein;
- 18           b. A judgment in favor of Plaintiff and the Class awarding them  
19           appropriate monetary relief, including actual damages,  
20           restitution, attorney fees, expenses, costs, and such other and  
21           further relief as is just and proper.
- 22           c. An order providing injunctive and other equitable relief as  
23           necessary to protect the interests of the Class and the general  
24           public as requested herein, including, but not limited to:
  - 25           i. Ordering that Defendant engage third-party security  
26           auditors/penetration testers as well as internal security  
27           personnel to conduct testing, including simulated attacks,  
28           penetration tests, and audits on Defendant's systems on a

periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

- ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
- iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;
- v. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;
- vi. Ordering that Defendant conduct regular database scanning and securing checks;
- vii. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- viii. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

- 1 d. An order requiring Defendant to pay the costs involved in
- 2 notifying the Class Members about the judgment and
- 3 administering the claims process;
- 4 e. A judgment in favor of Plaintiff and the Class awarding them
- 5 pre-judgment and post-judgment interest, reasonable attorneys'
- 6 fees, costs and expenses as allowable by law; and
- 7 f. An award of such other and further relief as this Court may deem
- 8 just and proper.

9 **VIII. DEMAND FOR JURY TRIAL**

10 Plaintiff demands a trial by jury on all issues so triable.

11 DATED: August 21, 2023

12 Respectfully Submitted,

13 /s/ John J. Nelson  
14 John J. Nelson (SBN 317598)  
15 **MILBERG COLEMAN BRYSON**  
16 **PHILLIPS GROSSMAN, LLC**  
17 280 S. Beverly Drive  
18 Beverly Hills, CA 90212  
19 Tel: (858) 209-6941  
20 Email: jnelson@milberg.com

21 William B. Federman\*  
22 **FEDERMAN & SHERWOOD**  
23 10205 N. Pennsylvania Ave.  
24 Oklahoma City, OK 73120  
25 Telephone: (405) 235-1560  
26 Email: wbf@federmanlaw.com

27 \**Pro Hac Vice application to be submitted*

28 ***Counsel for Plaintiff and the Proposed***  
***Class***